PT0-003$^{\text{Q\&As}}$

CompTIA PenTest+

QUESTION 1

During an assessment, a penetration tester was able to access the organization\\'s wireless network from outside of the building using a laptop running Aircrack-ng. Which of the following should be recommended to the client to remediate this issue?

A. Changing to Wi-Fi equipment that supports strong encryption

B. Using directional antennae

C. Using WEP encryption

D. Disabling Wi-Fi

Correct Answer: A

If a penetration tester was able to access the organization\\'s wireless network from outside of the building using Aircrack-ng, then it means that the wireless network was not secured with strong encryption or authentication methods. Aircrackng is a tool that can crack weak wireless encryption schemes such as WEP or WPA-PSK using various techniques such as packet capture, injection, replay, and brute force. To remediate this issue, the client should change to Wi-Fi equipment that supports strong encryption such as WPA2 or WPA3, which are more resistant to cracking attacks. Using directional antennae may reduce the signal range of the wireless network, but it would not prevent an attacker who is within range from cracking the encryption. Using WEP encryption is not a good recommendation, as WEP is known to be insecure and vulnerable to Aircrack-ng attacks. Disabling Wi-Fi may eliminate the risk of wireless attacks, but it would also eliminate the benefits of wireless connectivity for the organization.

QUESTION 2

A penetration tester is testing a new version of a mobile application in a sandbox environment. To intercept and decrypt the traffic between the application and the external API, the tester has created a private root CA and issued a certificate

from it. Even though the tester installed the root CA into the trusted stone of the smartphone used for the tests, the application shows an error indicating a certificate mismatch and does not connect to the server.

Which of the following is the MOST likely reason for the error?

A. TCP port 443 is not open on the firewall

B. The API server is using SSL instead of TLS

C. The tester is using an outdated version of the application

D. The application has the API certificate pinned.

Correct Answer: D

This is the most likely reason for the error because the application is unable to validate the certificate issued by the tester\\'s private root CA. Certificate pinning is a process where an application compares the certificate presented by the server with a predefined set of certificates and only accepts connections if the presented certificate is one of the predefined certificates. This means that the application will reject any certificate that is not in the predefined set, even if it is valid.

QUESTION 3

During the reconnaissance phase, a penetration tester collected the following information from the DNS records:

A-----> www

A-----> host

TXT --> vpn.comptia.org

SPF---> ip =2.2.2.2

Which of the following DNS records should be in place to avoid phishing attacks using spoofing domain techniques?

A. MX

B. SOA

C. DMARC

D. CNAME

Correct Answer: C

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps prevent email spoofing and phishing. It builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified

Mail) to provide a mechanism for email senders and receivers to improve and monitor the protection of the domain from fraudulent email.

Understanding DMARC:

Implementing DMARC:

Benefits of DMARC:

DMARC Record Components:

Real-World Example:

References from Pentesting Literature:

Step-by-Step ExplanationReferences:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 4

A penetration tester needs to identify all vulnerable input fields on a customer website. Which of the following tools would be best suited to complete this request?

A. DAST

B. SAST

C. IAST

D. SCA

Correct Answer: A

Dynamic Application Security Testing (DAST):

Advantages of DAST:

Examples of DAST Tools:

Pentest References:

Web Application Testing: Understanding the importance of testing web applications for security vulnerabilities and the role of different testing methodologies.

Security Testing Tools: Familiarity with various security testing tools and their applications in penetration testing.

DAST vs. SAST: Knowing the difference between DAST (dynamic testing) and SAST (static testing) and when to use each method. By using a DAST tool, the penetration tester can effectively identify all vulnerable input fields on the customer

website, ensuring a thorough assessment of the application\\'s security.

QUESTION 5

Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning

B. Shoulder surfing

C. Tailgating

D. Site survey

Correct Answer: C

Understanding Tailgating:

Methods to Prevent Tailgating:

Examples in Penetration Testing:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups